No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
A1, M1, O1, or T1	Include a description of the vulnerability to the system, how vulnerability was discovered, and source requirement.	Natural, Environmental, Human or Administrative; identify specific agents within the category.	H/M/L	Criticality rating/ Sensitivity rating (include which CIA was used)	H/M/L and why (ex. if environmental, # times threat occurred in past year)	H/M/L and why (list associated counter-measures)	H/M/L (based on Capability vs. Counter-measure matrix)	H/M/L (based on Impact vs. Likelihood matrix)	Prioritize within MOTA - based on risk and sense of immediacy	List proposed measures to mitigate the identified risk.
M1	**Security testing of changes is not part of the CDDTS configuration management plan.** Functional testing of security features is part of testing procedures, but vulnerability testing, penetration testing, system scanning, and network scanning is not a defined element of the configuration management plan. Details of application security testing were not directly evaluated, but test plans covered functional testing and did not specify security code reviews and testing for issues such as buffer overflows. BLSR 45. Systems should be thoroughly tested according to accepted standards and moved into a secure production environment through a controlled process (NIST: Executive Guide to the Protection of Information Resources); BLSR 53. All applications are tested for input boundary conditions to prevent buffer overflows and other privileged access. (GBP) BLSR 79. Establish technical controls to ensure appropriate security controls are specified, designed into, tested and accepted in the application in accordance with NIST guidance (OMB Circular A-130 Appendix III, Section A-3,	Human (denial of service, falsified data, fraud, hacking, malicious code, password guessing, sabotage, system tampering, unauthorized disclosures)	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Medium - network access is limited to internal users. However, CDDTS components may be subject to many types of popular attacks on web technology components that have not been tested.	High - limited access to CDDTS helps limit external attacks, but does not remove the ability of insiders or skilled attackers who could use other connected servers to launch attacks based on known vulnerabilities in web application components.	Low	Medium	1	Test CDDTS components using vulnerability and applications scanning techniques designed for web applications.

No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
M2	**Anti-virus tools are not run on the CDDTS server.** Anti-virus tools are run on the administrator and developer workstations used for CDDTS, but not the CDDTS server. BLSR 39. LAN servers should be scanned by the area responsible for LAN management to assure no virus becomes resident on the LAN server (FIPS PUB 191, Appendix A, 4.LA4)	Human - proliferation of malicious code (viruses, worms, trojans, etc.)	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Medium - the CDDTS system is not directly available to users via the Internet, and current administrative and development users connect from workstations running antivirus tools. (NOTE: if antivirus tools are NOT installed on the workstations of CDDTS operational users, the capability rating may be High.)	High - administrative users and developers have antivirus tools installed on their workstations. (It is not known whether operational CDDTS users also have antivirus tools installed.) However, the CDDTS production server is connected to an internal network segment that houses other servers that could provide in infection route.	Low	Medium	2	Deploy virus detection software on the CDDTS servers.
M3	**Security training during employee orientation is brief and not documented.** CDDTS security policy and procedures are addressed only briefly during ACS new employee orientation. The security topics that are addressed should be documented to help demonstrate that security issues relevant for new users are covered adequately. BLSR 8. OPM regulation requires training for new employees within 60 days of hire. (Practices for Securing Critical Information Assets, p.6); also see BLSR # 9, 11, 12, 13, 14. BLSR 11. Computer security training should be implemented into existing training programs such as orientation programs for new employees, and training courses involved with information technology systems equipment and software packages (FIPS PUB 191, Appendix A GP9) BLSR 13. OPM regulation requires training when an employee enters a new position that deals with sensitive information. (Practices for Securing Critical Information Assets, p.6) BLSR 14. OPM regulation requires refresher courses based on the sensitivity of the information the employee handles. (Practices for Securir	Human - Inadequately trained users could, through lack of knowledge about security policy and security controls, misuse the system or allow others to commit acts such as impersonation, hacking, guessing of weak passwords, disclosing or changing sensitive information, or propagating malicious code (viruses, worm, trojans, etc.)	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Low - there are a limited number of CDDTS users, and no access to the system is allowed through public networks.	Medium - training can prevent many, but not all, security problems due to lack of knowledge about proper use of system facilities and security controls.	Low	Medium	3	Document the security topics covered and the time devoted to them during employee orientation.

No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
M4	**Disaster recovery plans have not been tested.** A plan for disaster recovery and business continuity has been developed but has not yet been tested. Testing is scheduled for mid-September. BLSR 19. Establish continuity of support to periodically test the capability to provide continual service to users within a system (OMB Circular A-130 Appendix III, Section A-3, a.2.e, Section B-a.2.e)	Natural (all types), Environmental (all types)	Medium	Criticality - Mission Important Sensitivity - Availability (Medium)	Medium - Ocurrance of environmentat and natural threats has been relatively low, but without testing, the adequacy of the existing disaster recovery plan can not be assessed. Power outages and fluctuations occur several times a year, but they are handled adequately by the UPS and generator system.	Low - the effectiveness of the current disaster recovery plan cannot be assessed until it is tested.	Medium	Medium	4	Test the business continuity plan. Testing is currently planned for September.
M5	**Business continuity plans have not been tested.** Business continuity plans are in place but have not yet been tested. Testing is scheduled for mid-September. BLSR 20. Areas of control will include continuity of service operations. (Practices for Securing Critical Information Assets, p.18); BLSR 21. Establish contingency planning to periodically test the capability of the major application to perform and function in event of failure of its automated support (OMB Circular A-130 Appendix III, Section A-3, b.2.d)	Natural (all types), Environmental (all types)	Medium	Criticality - Mission Important Sensitivity - Availability (Medium)	Low - Ocurrance of environmentat and natural threats has been relatively low, but without testing, the adequacy of the existing business continuity plan cannot be assessed. Power outages and fluctuations occur several times a year, but they are handled adequately by the UPS and generator system.	Low - the effectiveness of the current business continuity plan cannot be assessed until it is tested.	Low	Medium	5	Test the disaster recovery plan. Testing is currently planned for September.

No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
M6	**A security training and awareness program has not been fully implemented.** A security training and awareness program was being developed at the time this assessment was conducted. The program is planned for deployment in the near future. BLSR 7. Provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency (OMB Circular A-130 Appendix III, Section A-3, a.2.b, b.2.b, Section B-a.2.b, b.2.b; Computer Security Act of 1987, Section 5.a)	Human - Inadequately trained users could, through lack of knowledge about security policy and security controls, misuse the system or allow others to commit acts such as impersonation, hacking, guessing of weak passwords, disclosing or changing sensitive information, or propagating malicious code (viruses, worm, trojans, etc.)	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Low - there are a limited number of CDDTS users, and no access to the system is allowed through public networks.	Medium - training can prevent many, but not all, security problems due to lack of knowledge about proper use of system facilities and security controls.	Low	Medium	6	Implement the planned security awareness training program; document the topics covered to demonstrate the effectiveness of the training program; maintain records of training for each user to demonstrate that all users have completed required training.
M7	**Several critical security services are performed for CDDTS by contractor divisions that may be acquired by a third party.** Security services provided now by the ACS Security Organization (as described in BLSR 18) or the ACS Defense Division (as described in BLSRs 27-29) may not be available if part of ACS is acquired by a third-party (as recently announced). BLSR 18. Establish an incident response capability to provide help to users when a security incident occurs (OMB Circular A-130 Appendix III, Section A-3, a.2.d Section B-a.2.d, Practices for Securing Critical Information Assets, p.47, Presidential Decision Directive-PDD 63); BLSR 27. Vulnerabilities assessments (reviews to identify existing weaknesses but not to determine if all requirements are met) of all assessable units (i.e., computer system or application) shall be performed, at a minimum, every three years. (OMB A-123, 6, 8c); BLSR 28. A vulnerability audit will be performed to find and document the vulnerabilities in critical information assets. (Practices for Securing Critical Information Assets, p.17); BLSR 29. Perform risk assessment to inc	Human - vulnerabilities and attacks on CDDTS may not be detected in timely manner, creating the opportunity for unauthorized use, denial of service, browsing of Privacy Act data, falsified data input, fraud, hacking, impersonation, interception, introduction of malicious code, sabotage, spoofing, system tampering, or unauthorized disclosure of sensitive information.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Low - access to CDDTS through the network is restricted to internal ACS and Call Center users.	Medium - physical access is restricted to ACS facilities that can access CDDTS.	Low	Medium	7	Monitor acquisition of ACS components; if necessary, contract for intrusion detection, vulnerability assessment, and penetration testing of CDDTS components. NOTE: If these security monitoring services are no longer available, the Capability rating would change to Medium, Likelihood would change to Medium, and the Risk rating would change to High.

No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
M8	**Security risk analysis and testing is not included in the configuration management plan.** There is a detailed configuration management process defined for CDDTS, which includes an Impact Analysis. However, a security risk analysis is not an explicit part of the impact review. (No major changes or upgrades have been made to CDDTS since October 2002, with the Phase III release.) BLSR 26. A risk analysis shall be performed whenever there is a significant change to the installation. A significant modification made to an SBU AIS or network shall require a review to determine the impact on the security of the processed SBU information. (OMB A-130, III-4, 3.c.2.b)	Human - since this is the first risk assessment has been conducted, there is no baseline against which to measure the adequacy of security controls for preventing compromise of system function and data confidentiality. Administrative - OIG review of the system could lead to an audit finding that CDDTS has been operational for a year without having a risk assessment performed.	Medium	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Low - the current assessment will address the effectiveness of existing controls and recommend counter-measures for security issues that are discovered.	High	Low	Low	8	A schedule for periodic risk assessments should be developed for CDDTS. Any short-term issues that arise because of not having a security risk assessment can be addressed by referring to the current assessment.
M9	**Off-site storage of back-up media and business continuity locations are relatively close to the primary CDDTS Data Center.** Offsite storage, business continuity sites, and disaster recovery data centers are in the local area (i.e., <300 miles) so major disasters (e.g., hurricanes, terrorist attacks) could affect both the data center and the backup site. BLSR 42. Off-site facilities should be sufficiently distant from the operating facility to provide adequate protection against major natural disasters (e.g. earthquakes and hurricanes) (GBP)	Natural (storm damage, earthquakes), Environmental (Long-term power failure, biological/chemical terrorism)	Medium	Criticality - Mission Important Sensitivity - Integrity (Medium), Availability (Medium)	Medium - historical experience would indicate that effects of the stated threats would typically be limited geographically.	High - offsite storage provides protection against many types of natural and environmental disasters, and the probability that the offsite storage location and the CDDTS data center would be simultaneously affected are relatively small.	Low	Low	9	Consider offsite storage locations that are more distant from the CDDTS data center.

No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
O1	**Authorized access is not reviewed annually.** A procedure for annual review and certification of CDDTS users is not defined in the System Security Plan. BLSR 108. The list of persons with authorized access should be reviewed and recertified annually (GBP)	Human - users may retain access to CDDTS after they leave job positions that require access, leading to unauthorized use, denial of service, browsing of Privacy Act data, falsified data input, fraud, hacking, impersonation, interception, introduction of malicious code, sabotage, spoofing, system tampering, or unauthorized disclosure of sensitive information.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Low - access through the network is restricted to internal users, so an unauthorized user who retains an account on the CDDTS application would need to log in from an internal network location or from the ACS Call Center.	Medium - physical access is restricted to ACS facilities that can access CDDTS.	Low	Medium	1	Implement procedures and tools to detect users who no longer need CDDTS access and disable their accounts.
T1	**Audit trail logging and review are not routinely performed.** User activity is not logged, although logs are maintained for IDS data and operating system-level security events. BLSR 95. The system shall be able to create, maintain, and protect from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects (GBP) BLSR 96. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and the success or failure of the event (GBP); BLSR 97. The area responsible for LAN management should conduct timely audits of LAN server logs (FIPS PUB 191, Appendix A, 3. NM6); BLSR 99. The security administrator will review reports to determine if there have been repeated unsuccessful attempts to login to the network (GBP)	Human - attacks on CDDTS may not be detected in timely manner, creating the opportunity for unauthorized use, denial of service, browsing of Privacy Act data, falsified data input, fraud, hacking, impersonation, interception, introduction of malicious code, sabotage, spoofing, system tampering, or unauthorized disclosure of sensitive information.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Medium - access throiugh the network is restricted.	Medium - the Intrusion Detection System being deployed will help detect potential attacks; however, the IDS must also be monitored and reviewed to provide benefits.	Medium	High	1	Record user activity in audit logs; provide processes and tools for frequent review and monitoring of audit logs, firewall logs, IDS logs, and system logs.

No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
T2	**User passwords for the CDDTS application are stored in clear text.** User passwords are stored in an Oracle table in plain text. Administrative users with access to the password table could perform actions as if they were an operational user without detection, compromising accountability of individual users. BLSR 54. Passwords shall be encrypted (GBP); BLSR 86. Passwords must be stored with one-way encryption (GBP); BLSR 87. No one but the user ID owner can have the ability to know or view passwords (GBP)	Human - compromise of user acountability that can lead to many types of compromise: unauthorized browsing of privacy data, corrupted data input, fraud, hacking, impersonation, spoofing, system tampering, theft, unauthorized disclosure.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Medium - network access is limited to internal users.	Low - there are few mitigating controls, such as user activity auditing that could detect unauthorized use of passwords.	Medium	High	2	Store user passwords as one-way hashes using any of the well known and effective hashing algorithms. Implement user activity auditing to track user actions and to maintain user accountability.
T3	**There are no functions to detect and lock accounts after repeated login failure.** Security functions for account lock-out and or ID revocation after multiple failed login attempts are not described in the CDDTS system security plan or CDDTS design documentation. BLSR 83. The system shall support a lock-out threshold if excessive invalid access attempts are input (GBP) BLSR 84. User IDs must be revoked if a password attempt threshold of three failed login attempts is exceeded (GBP)	Human - by not monitoring failed login attempts, it would be possible for an attacker to repeatedly attempt to log in to CDDTS and guess a user's password; successful attacks could lead to browsing of Privacy Act data, falsified data input, fraud, hacking, impersonation, interception, introduction of malicious code, sabotage, spoofing, system tampering, or unauthorized disclosure of sensitive information.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Medium - network access to CDDTS is restricted to internal users.	Medium - there are some limited auditing mechanisms for tracking CDDTS system usage, but logs are only reviewed when a security incident or system problem is suspected.	Medium	High	3	Implement a system lock-out function for failed login attempts that exceed a defined number. Increase the log review frequency or implement other forms of security monitoring to improve the probability of detecting attacks.

No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
T4	**The System Security Plan does not specify periodic scanning for unauthorized modems.** Scanning for unauthorized modems was not included in this assessment and should be part of periodic vulnerability analyses. BLSR 61. Do not leave personal computers containing sensitive data which are connected to answering modems unattended (GBP)	Human - unauthorized modems can result in system compromise, unauthorized browsing of data, falsified data input, fraud, hacking, password guessing, sabotage, spoofing, unauthorized disclosure of sensitive information, and implanting of malicious code.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Medium - exploiting unauthorized modems to access CDDTS would bypass the network controls that are supposed to limit access to internal users. CDDTS is connected to the internal ACS LAN, so modems connected on the LAN could potentially gain access to the CDDTS server.	Medium - Access controls in the CDDTS application and the CDDTS database would limit the ability of attackers to easily gain access to CDDTS data or system components.	Medium	High	4	Vulnerability testing should ijnclude scanning for unauthorized modems. NOTE: If scanning for unauthorized modems has been included in past vulnerability assessments, the Countermeasures rating would change to High, the Likelihood would change to Low, and the Risk rating would change to Medium.
T5	**An Intrusion Detection System is not yet fully implemented.** Intrusion detection system (IDS) sensors are in the process of being deployed but are not yet fully operational. IDS monitoring is provided by the ACS Defense Division. A related question to address is who will provide these services if the ACS Defense Division is acquired by a third-party (as recently announced). BLSR 66. Intrusion detection systems (IDS) will be used to: Monitor and analyze user and system activity; Assess the integrity of critical system and data files; Recognize activity patterns involved in known attacks; Perform statistical analyses to spot abnormal activity patterns that may indicate an attack; Manage the operating system audit trail and alert system managers to user behavior (Practices for Securing Critical Information Assets, p.36)	Human - unauthorized and undetected access to the CDDTS network and servers could result in denial of service attacks, system compromise, unauthorized browsing of data, falsified data input, fraud, hacking, password guessing, sabotage, spoofing, unauthorized disclosure of sensitive information, and implanting of malicious code.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Medium - network access to CDDTS is restricted to internal users.	High - an Intrusion Detection System is being deployed. However, it will be operated by the ACS Defense Division, which may be acquired by a third party organization. In that case, the plans for operation of an intrusion detection capability will need to be reassessed.	Low	Medium	5	Track completion progress of the ACS Intrustion Detection System for CDDTS. Follow progress of any changes in ownership of the ACS Defense Division to make sure intrustion detection capabilities are maintained and appropriately monitored. Deploy host intrusion detection software on the CDDTS server (e.g., Tripwire) to detect unauthorized changes in CDDTS application or operating system components.

No.	Vulnerability	Threat	Impact	Impact Calculation	Capability	Effective Counter-measures	Likelihood	Risk	Priority	Proposed Countermeasures
T6	**Firewall policies and filtering rules should be audited.** Firewall filtering rules and policies are being put in place for CDDTS in response to an OIG audit of DLSS. They were not assessed during this review. BLSR 74. Inbound filtering will be performed to exclude or reject all data packets that have an internal host address (GBP)	Human - inappropriate configuration of firewalls could lead to several types of system compromise, including denial of service attacks, system compromise, unauthorized browsing of data, falsified data input, fraud, hacking, password guessing, sabotage, spoofing, unauthorized disclosure of sensitive information, and implanting of malicious code.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Medium - network access to CDDTS is restricted to internal users.	High - Vulnerability scanning has been performed by ACS personnel.	Low	Medium	6	Future security assessments should include analysis of firewall rule sets and firewall policies.
T7	**CDDTS accounts are not configured for automatic logout after periods of inactivity.** Automatic logout is not defined in the CDDTS system design or CDDTS system security plan. BLSR 90. Terminals, workstations, and networked personal computers should never be left unattended when user ID and password have been logged in (GBP); BLSR 94. Where appropriate, terminals/ workstations should automatically log out if inactive for a specified period of time (GBP)	Human - users may leave workstations logged on an connected to CDDTS, creating the opportunity for unauthorized use, resulting in browsing of Privacy Act data, falsified data input, fraud, hacking, impersonation, interception, introduction of malicious code, sabotage, spoofing, system tampering, or unauthorized disclosure of sensitive information.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Low - there are a limited number of CDDTS users, and they are all internal, either at the ACS Call Center or within ACS user areas.	High - user areas have controlled access, limiting physical access of potential attackers to workstations logged in to CDDTS.	Low	Medium	7	Implement an automatic logout system.
T8	**Some file transfers to CDDTS are made through standard FTP.** File transfers are via direct connection to DLSS or FTP. FTP controls should be defined to protect transmitted data, or a secure form of file transfer (e.g., a secure FTP product, or encryption of files before transmission) should be used if files are transmitted over public networks. BLSR 68. Sensitive data files should be protected during transmission from one location to another (GBP)	Human - unauthorized access to CDDTS files could result in unauthorized browsing of data, falsified data input, fraud, hacking, sabotage, spoofing, unauthorized disclosure of sensitive information, and implanting of malicious code.	High	Criticality - Mission Important Sensitivity - Confidentiality (High), Integrity (Medium), Availability (Medium)	Low - file transfers take place on a relatively infrequent basis, and are transmitted via internal network segments.	Medium - FTP transfers take place over internal networks.	Low	Medium	8	Use encryption or a secure FTP tool to transfer files to CDDTS. NOTE: If any FTP transfers take place over the Internet, the Capability rating would be Medium, the Likelihood would change to Medium, and the risk would change to High.